WHAT IS CLAIMED IS:

Encryption:

1.   A method, comprising:

        obtaining a hint;

        obtaining a password;

        performing a hashing algorithm on the hint and the password to generate a key;

        encrypting data using the key; and

        sending the encrypted data to a server for storage.

2.   The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password.

3.   The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key.

1   4.   A system, comprising:

2   a user interface for obtaining a password;

3   a key generator coupled to the user interface for performing a hashing

4   algorithm on a hint and the password to generate a key;

5   an encryption engine coupled to the key generator for encrypting data using

6   the key; and

7   a communications module coupled to the engine for sending the encrypted

8   data to a server for storage.

1   5.   The system of claim 4, further comprising a hint generator for generating

2   the hint.

1   6.   The system of claim 4, wherein the key generator hashes the password.

1   7.   The system of claim 4, wherein the key generator hashes the password to

2   derive a first secret, hashes the first secret to derive a second secret, hashes the hint

3   and the first secret to generate an intermediate index, and hashes the intermediate

4   index and the second secret to generate the key.

1   8.   A system, comprising:

2   means for obtaining a hint;

3   means for obtaining a password;

4   means for performing a hashing algorithm on the hint and the password to

5   generate a key;

6   means for encrypting data using the key; and

7   means for sending the encrypted data to a server for storage.

1   9.   The system of claim 8, wherein the system includes code stored on a

2   computer-readable storage medium.

1   10.   The system of claim 8, wherein the system includes code embodied in a

2   carrier wave.

1   11.   A method, comprising:

2   receiving a request to store encrypted data from a client;

3   sending an encryption downloadable for deriving a key to encrypt data to

4   the client;

5   receiving encrypted data that was encrypted by the encryption

6   downloadable from the client; and

7   obtaining a hint, corresponding to the encrypted data and needed for

8   regenerating the key; and

9   storing the hint and the encrypted data.

1   12.   A system, comprising:

2   an encryption downloadable for deriving an encryption key from a

3   password and a hint;

4   a web server for interfacing with a client, for sending the encryption

5   downloadable to the client, and for receiving encrypted data that was encrypted by

6   the encryption downloadable from the client; and

7   memory coupled to the web server for storing a hint corresponding to the

8   encrypted data and needed to regenerate the key from the client and the encrypted

9   data.

1 Client-side decryption

2 13.   A method, comprising:

3   obtaining a password;

4   receiving encrypted data and a hint corresponding to the encrypted data

5 from a server; and

6   performing a hashing algorithm on the password and the hint to generate a

7 key for decrypting the encrypted data.

1 14.   The method of claim 13, wherein the step of performing a hashing

2 algorithm includes hashing the password.

1 15.   A system, comprising:

2   a user interface for obtaining a password;

3   a communications module for receiving the encrypted data and a hint

4 corresponding to the encrypted data from a server;

5   a key generator for performing a hashing algorithm on the password and the

6 hint to generate a key for decrypting the encrypted data.

1 16.   A system, comprising:

2   means for obtaining a password;

3   means for receiving encrypted data and a hint corresponding to the

4 encrypted data from a server; and

5   means for performing a hashing algorithm on the password and the hint to

6 generate a key for decrypting the encrypted data.

1 17.   The system of claim 16, wherein the system includes code stored on a

2 computer-readable storage medium.

1   18.   The system of claim 16, wherein the system includes code embodied in a

2   carrier wave.

1   19.   A method, comprising:

2   receiving identification of encrypted data;

3   sending a decryption downloadable for deriving a key from a password and

4   a hint to a client; and

5   sending a hint corresponding to the encrypted data to the client.

1   20.   A system, comprising:

2   a decryption downloadable for deriving a key from a password and a hint;

3   encrypted data;

4   a hint corresponding to the encrypted data; and

5   a web server for interfacing with a client, and for sending the decryption

6   downloadable, the encrypted data and the hint to the client.

1   Server-side decryption

2   21.   A client-based method, comprising:

3   obtaining a password;

4   deriving a first secret from the password;

5   receiving a hint corresponding to data to be decrypted from a server;

6   deriving an intermediate index from the first secret and the hint; and

7   sending the intermediate index to the server.

1   22.   The method of claim 21, wherein deriving the first secret includes hashing

2   the password.

1   23.   The method of claim 21, wherein deriving an intermediate index includes

2   hashing the first secret and the hint.

1   24.   A system, comprising:

2   a user interface for obtaining a password;

3   an index generator coupled to the user interface for generating an

4   intermediate index from a hint received from a server and a secret derived from the

5   password; and

6   a communications engine coupled to the index generator for sending the

7   intermediate index to the server.

1   25.   The system of claim 24, wherein the index generator generate the

2   intermediate index by hashing the hint and the secret.

1   26.   A system, comprising:

2   means for obtaining a password;

3   means for deriving a first secret from the password;

4   means for receiving a hint corresponding to data to be decrypted from a

5   server;

6   means for deriving an intermediate index from the first secret and the hint;

7   and

8   means for sending the intermediate index to the server.

1   27.   The system of claim 26, wherein the system includes code stored on a

2   computer-readable storage medium.

1   28.   The system of claim 26, wherein the system includes code embodied in a

2   carrier wave.

1   29.   A server-based method, comprising:

2   receiving an indication of encrypted data to be decrypted;

3   transmitting to a client a hint corresponding to the indication, and a

4   decryption downloadable for deriving an intermediate index from a password and

5   the hint;

6   receiving the intermediate index from the client; and

7   deriving a decryption key from a second secret corresponding to the user

8   and the intermediate index.

1   30.   A system, comprising:

2   a second secret corresponding to a user;

3   a decryption downloadable for generating an intermediate index from a

4   password and a hint;

5   a web server for receiving an indication of encrypted data to be decrypted,

6   for transmitting the decryption downloadable and a hint corresponding to the

7   indication to a client, and for receiving an intermediate index from the client; and

8   a server-resident module for deriving a key for decrypting the encrypted

9   data from the second secret and the intermediate index.